The licensing terms at https://www.adp.com/WorkforceManagerTerms shall apply for all agreements or amendments for ADP Workforce Manager Services signed on or after October 1, 2025, and the terms below will not apply.

The following licensing terms shall apply for all agreements or amendments for ADP Workforce Manager Services signed prior to October 1, 2025.

Article 1. The Services

1.1 The ADP® Workforce Manager Services (the "WFM Services") that are the subject of these Additional Terms Applicable to ADP® Workforce Manager Services (this "Exhibit") are described throughout this Exhibit and at the following Attachments:

Attachment 1: Workforce Manager Cloud Guidelines

Attachment 2: Acceptable Use Policy ("AUP")

Attachment 3: Data Protection Attachment ("DPA")

Attachment 4: Security Measures

1.2 Client's Authorized Users may access the WFM Services on behalf of Client. "Client's Authorized Users" are any individual or entity that directly (or through another one of Client's Authorized Users) accesses or uses the WFM Services by virtue of any login credentials or passwords Client uses to access the WFM Services. Client is responsible for all actions taken by Client's Authorized Users. Client will ensure that Client's Authorized Users comply with Client's obligations under this Agreement, including without limitation ensuring that such Authorized Users are under obligations of confidentiality pursuant to a written agreement. Unless ADP breaches its obligations under this Agreement, ADP is not responsible for unauthorized access to Client's account, nor activities undertaken with Client's login credentials, nor by Client's Authorized Users. Client should contact ADP immediately if Client believes an unauthorized person is using Client's account or that Client's account information has been compromised.

1.3 If any terms set forth in this Exhibit conflict with terms set forth in the Agreement, the terms set forth in this Exhibit shall prevail.

Article 2. Information, Confidentiality, Security and Privacy

Section 2.1 Certain Uses

2.1.1 "Client Data" is any content that Client or Client's Authorized Users post to or input into the WFM Services. Client owns Client Data. Client is solely responsible for Client Data, including ensuring that Client Data complies with the Acceptable Use Policy (AUP) and all applicable laws and regulations.

2.1.2 Client agrees that Client Data shall not include categories of data fields that are not required for the provision of the WFM Services, including but not limited to the following types of data: financial account numbers linked to an individual; payment card information; medical records or heath data relating to an individual; any records from a US or non-US consumer reporting agency (including, for example, credit reports) and any data falling within the definition of "Special Category Data" pursuant to the EU General Data Protection Regulation (EU/2016/679) unless required for the WFM Services. ADP and its subcontractor, Kronos Incorporated ("Subcontractor"), do not accept responsibility for Client´s use of the aforementioned categories of data that are the subject of a post or input to the WFM Services.

Section 2.2 Security and Privacy

ADP or Subcontractor, on the one hand, and Client on the other hand, shall each comply with their respective obligations pursuant to Attachment 3 ("Data Protection Attachment"), which is an integral part of the Agreement between Client and ADP for the WFM Services. In the case of any conflict or inconsistency between the terms of the Agreement and the terms of Attachment 3 with respect to data protection or security, the terms of Attachment 3 shall prevail.

Article 3. Warranty

ADP warrants during the term of the Agreement that the WFM Services, under normal operation as specified in the published documentation for the WFM Services, and when used as authorized under the Agreement, will perform substantially in accordance with such documentation. ADP DISCLAIMS ALL OTHER WARRANTIES ON THE WFM SERVICES, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Article 4. License

4.1 As part of the WFM Services, ADP will provide Client access to and use of various technologies ("Technology"). ADP or our Subcontractor own all title or possess all intellectual property rights in and to the Technology used in delivering the WFM Services. Client has a right to use this Technology subject to this Agreement and solely to receive the WFM Services. No other use of the Technology is permitted. Client is specifically prohibited from reverse engineering, disassembling or decompiling the Technology, or otherwise attempting to derive the source code of the Technology. Client may not contact third party

licensors or suppliers, including without limitation our Subcontractor, for direct support of the Technology.

4.2 The WFM Services do not include development tools for the Boomi AtomSphere Service, even if access to the Boomi AtomSphere Service by Client is possible, Client may not use administrative rights to log in to the Boomi AtomSphere Service for purposes of utilizing design and development tools.

Article 5. Suspension

Client is responsible for Client's and Client's Authorized User's compliance with the AUP. ADP and our Subcontractor reserve the right to review Client's use of the WFM Services and Client Data for AUP enforcement. If ADP or our Subcontractor discover an AUP violation, and it is reasonably determined that immediate action must be taken to prevent further harm, the WFM Services may be suspended immediately without notice. In such event, ADP will promptly contact Client to discuss the violation and steps needed to remedy the violation so that the WFM Services may be restored as soon as possible. If ADP or our Subcontractor determines that the violation does not require suspension, ADP will notify Client of the AUP violation and discuss remediation steps.

Article 6. Effects of Termination

If the WFM Services are terminated in accordance with the terms of the Agreement:

a. Client's right to use the WFM Services will end as of the effective date of termination, but Client will have thirty (30) days after the effective date of termination to access the WFM Services for purposes of retrieving Client Data through tools that will enable Client to extract Client Data. If Client requires longer access to the WFM Services after the 30th day following the effective date of termination to retrieve Client Data from time to time, such access will be subject to additional fees and otherwise subject to the terms of this Agreement.
b. Client Data will be deleted after Client's rights to access the WFM Services and retrieve Client Data have ended. Client Data will be deleted in a series of steps in accordance with our Subcontractor's standard business practices, including system backups. Final deletion of Client Data will be completed when the last backup that contained Client Data is overwritten.
c. Provisions in this Exhibit which by their nature are intended to survive in the event of a dispute or because their obligations continue past termination of the Exhibit will so survive.

Attachments to Exhibit 1

Attachment 1: ADP® WORKFORCE MANAGER Cloud Guidelines

Attachment 2: Acceptable Use Policy

Attachment 3: Data Protection Attachment

Attachment 4: Security Measures

Always Designing for People™

ATTACHMENT 1
ADP Workforce Manager Cloud Guidelines

Solution Definition	
Tenants included	One standard product ion tenant One partial copy non-production tenant limited to 18 months of data
Additional tenants	Additional non-production partial copy tenants available for purchase invoiced monthly
Connectivity	
Connectivity to service	The Client's end users connect to WFM Services applications via a secure SSL/TLS connection over the internet. Cooperation between ADP and Client's IT staff may be required to enable access. ADP will assist with validating site connectivity but assumes no responsibility for the Client's internet connection or ISP relationships. ADP-related internet traffic cannot be filtered by proxy or caching devices on the client network. ADP Workforce Manager supports vanity URL, utilizing a single domain.
SFTP accounts	The ADP Workforce Manager cloud SFTP service provides a generic endpoint for Client to push and pull files —such as people import, payroll, accruals, schedules, punches, volume drivers, and more — to and from the ADP Workforce Manager cloud in support of Workforce Manager integrations. The service includes two SFTP managed service accounts that Client may use for integrations with the ADP Workforce Manager cloud. All managed service account logins use public key authentication to secure files in transit. Transfers of files up to 100MB are supported. Client may also purchase additional managed service accounts. User accounts for individual (named) Client login are not supported by the SFTP service.
Usage	
Secure file transfer limits	Integration with WFM Services using the Subcontractor Cloud SFTP service is subject to the following limits: - 20 active concurrent sessions per SFTP account - File size transferred per SFTP session not to exceed 100MB - Storage quota of 10GB per SFTP account The above are subject to change.
Key performance indicators (KPIs)	KPIs can be used to monitor and control business targets and thresholds. Many KPIs are delivered to the Client to track common workforce metrics such as overtime and labor costs. The Client has the option to build additional organization-specific KPIs using the KPI Builder. The number of active KPIs used with WFM Services applications will be limited to 200 per Client.
API usage	Data can be accessed through APIs. ADP and its Subcontractor reserves the right to limit usage of APIs to preserve the integrity of the system. Data usage limitations will be measured on a per-minute basis. The expected volume of API calls may be exceeded by building additional applications using APIs or routinely extracting large volumes of data to support an external data warehouse.
Policies	
Data refresh	Client can request that a copy of production tenant be moved to its non-production tenant no more than once per week — up to the limit of data allowable in the non-production tenant.
Application updates	Maintenance updates will be automatically applied as needed. New software releases will be automatically applied according to the release schedule when generally available to ADP clients.
Data retention	Customers can store production data during the Term, provided they perform "Payroll Signoff" per the product documentation. After the WFM Services are terminated, the terms of Article 6 (Effects of Termination) will apply.
Policies	
Termination support	Upon termination of the WFM Services, ADP will provide access to the service for an additional 30 days so the Client may extract data.
Disaster recovery	Recovery time objective: 24 hours

Encryption	Data encryption in transit and at rest is included.
Maintenance window	Four hours once a week, according to defined standard schedule, which is subject to change: Thursday, midnight – 4:00 a.m. EST
Policies	
Data usage	ADP or its Subcontractor has the right to use scrubbed system data to generally improve the look, feel and operating performance of the service.
Third parties	The Client may contract with a third party to configure and/or implement ADP Workforce Manager applications. The Client will be responsible for creating users in the system for the third party to access the application and for maintaining the permissions those users have within the application. Dedicated service and support accounts can be accessed only by ADP's or its Subcontractor's personnel or contractors.
Legal Hold	ADP or its Subcontractor will comply with applicable laws and regulations when responding to subpoenas and inquiries from government agencies after consultation with Clients when applicable and possible. In the event that Client is subject to a subpoena, litigation discovery request, or government inquiry directed at Client data or documents that are solely within the control of ADP or its Subcontractor, ADP or its Subcontractor will, at the Client's request, make commercially reasonable efforts to provide assistance to the extent that it is technically feasible. The Client will reimburse ADP or its Subcontractor for the costs that are incurred to provide such assistance, such as professional services fees, copying, delivery, and other handling expenses. Subject to the above, ADP or its Subcontractor will produce the relevant data or documents. Except at its sole discretion or if legally required to do so, ADP or its Subcontractor will not entertain requests to store or host legacy or archived Client data or documents for these purposes. ADP or its Subcontractor periodically reviews all matters subject to legal hold, including data that is being retained.

Always Designing for People™

ATTACHMENT 2

Acceptable Use Policy

This Acceptable Use Policy (this "Policy") describes prohibited uses of the Workforce Manager Services ("WFM Services"). The examples described in this Policy are not exhaustive. This Policy may be modified at any time upon written notice to Client. If Client violates the Policy or authorizes or helps others to do so, the WFM Services may be suspended until the violation is corrected, or the Agreement may be terminated for cause in accordance with the terms of the Agreement.

(a) No Illegal, Harmful, or Offensive Use or Content

Client may not use, or encourage, promote, facilitate or instruct others to use, the WFM Services for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include:

Illegal Activities. Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography.

Harmful or Fraudulent Activities. Activities that may be harmful to others, ADP's or our Subcontractor's operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.

Infringing Content. Content that infringes or misappropriates the intellectual property or proprietary rights of others.

Offensive Content. Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.

Harmful Content. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

(b) No Security Violations

Client may not use the WFM Services to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

Unauthorized Access. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System. Client will not perform any security integrity review, penetration test, load test, denial of service simulation or vulnerability scan on any System.

Falsification of Origin. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.

No Use of Robots. Client will not use any tool designed to automatically emulate the actions of a human user (e.g. robots) for the purposes of testing the WFM Service for load or stress testing, penetration testing, or other similar performance testing.

(c) No Network Abuse

Prohibited activities include:

Monitoring or Crawling. Monitoring or crawling of the WFM Services that impairs or disrupts the WFM Services.

Denial of Service (DoS). Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.

Intentional Interference. Interfering with the proper functioning of the WFM Services, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

Operation of Certain Network Services. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

Avoiding System Restrictions. Using manual or electronic means to avoid any use limitations placed on the WFM Services, such as access and storage restrictions.

(d) No E-Mail or Other Message Abuse

Client will not use the WFM Service to distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like “spam”), including commercial advertising and informational announcements. Client will not alter or obscure mail headers or assume a sender’s identity without the sender’s explicit permission. Client will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

(e) Monitoring and Enforcement

ADP and its Subcontractor, and Subcontractor’s third-party cloud service providers, reserve the right, but do not assume the obligation, to investigate any violation of this Policy or misuse of the WFM Services. ADP or its Subcontractor may:

- investigate violations of this Policy or misuse of the WFM Services; or
- remove, disable access to, or modify any content or resource that violates this Policy.

ADP or its Subcontractor may report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Such reporting may include disclosing appropriate Client information. ADP or its Subcontractor also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

(f) Reporting of Violations of this Policy

If Client becomes aware of any violation of this Policy, Client will immediately notify ADP and provide ADP with assistance, as requested, to stop or remedy the violation.

ATTACHMENT 3

Data Protection Attachment ("DPA")

1. ADP and its subcontractor, Kronos Incorporated ("Subcontractor") have implemented reasonable and appropriate administrative, physical, and technical safeguards designed to help Client secure Client Data against accidental or unlawful loss, access or disclosure, as set out in Attachment 4 ("Security Measures"). ADP and Subcontractor may change the Security Measures at any time without notice so long as they maintain a comparable or better level of security.
2. Each of Client, ADP and Subcontractor shall comply with all relevant and applicable laws governing their respective business. This includes, to the extent applicable, those laws and regulations pertaining to the processing of personal data and privacy in any relevant territory under this Exhibit ("Data Protection Laws").
3. This DPA does not apply to non-production environments of the WFM Services if such environments are made available by ADP to Client, and Client shall not store personal data in such environments.
4. ADP acts as a Processor, Subcontractor acts as a sub-processor, and Client and those Client group entities that Client permits to use the WFM Services act as Controllers under the DPA, and pursuant to the Agreement. Client acts as a single point of contact and is solely responsible for obtaining any relevant authorizations, consents and permissions for the processing of personal data in accordance with this DPA, including, where applicable approval by Controllers to use ADP as a Processor, and Subcontractor as a sub-processor. Where authorizations, consent, instructions or permissions are provided by Client these are provided not only on behalf of the Client but also on behalf of any other Controller affiliated with the Client and using the WFM Services.
5. Purpose of Processing. ADP and Subcontractor shall process the Client Data in accordance with Client´s instructions, as set out in the Agreement and as may documented in writing from time to time. ADP shall notify Client if ADP or Kronos consider an instruction from Client to be in violation of applicable Data Protection Laws, although a detailed legal examination will not be required.
6. Cooperation. At Client's request, ADP will reasonably cooperate with Client in dealing with requests from Client, Client data subjects or regulatory authorities regarding ADP's and Subcontractor´s processing of personal data or any personal data breach or for Client´s compliance with applicable Data Protection Laws. ADP shall notify the Client as soon as reasonably practical about any request it has received from a Client data Subject in relation to the personal data processing, without itself responding to such request without Client's further instructions, if applicable.
7. Personal Data Breach Notification. ADP will notify Client without undue delay after becoming aware of any personal data breach and provide reasonable information to assist Client to meet any Client obligations to report a personal data breach as required under applicable Data Protection Law. ADP may provide such information in phases as it becomes available.

8. International Transfers of Client Data. With respect to any Client Data that constitutes "personal information" pursuant to applicable Data Protection Laws and originating in any nation of the European Economic Area or Switzerland ("Client EEA Personal Data"), the following shall apply:
    a. ADP and Subcontractor shall ensure adequate protection for transfers of EEA Personal Data outside the EEA.
    b. ADP and Subcontractor shall be entitled to process Client EEA Personal Data, including by using sub-subprocessors, in accordance with this DPA outside the country in which the Client EEA Personal Data originated, as permitted by applicable Data Protection Laws.
    c. ADP and Subcontractor enter into the "processor – processor" EU-approved Standard Contractual Clauses for transfers subject to the European General Data Protection Regulation and/or the Swiss Federal Data Protection Act and the UK Addendum.
9. Subprocessors. ADP is granted a general authorisation for the further subcontracting for the processing of personal data by Subcontractor to Sub-subprocessors, provided that:
    (a) Subcontractor shall engage sub-subprocessors under a written (including in electronic form) contract consistent with the terms of this DPA in relation to the sub-subprocessor's processing of personal data. ADP shall be liable for any breaches by the sub-subprocessor in accordance with the terms of the Agreement;
    (b) the list of Sub-subprocessors in place on the effective date of the Agreement is attached hereto or made available to Client upon request, including the name, address and role of each Sub-subprocessor used to provide the WFM Services.
10. New subprocessors. Following the Effective Date, if Subcontractor intends to rely on a new sub-subprocessor for the processing of Client Data, then ADP shall provide Client with no less than 30 days´ prior notice. Client shall then have a period of 10 days to provide detailed written objections or seek further information regarding such intended new sub-subprocessor. In case of Client objections, the parties shall work in good faith to determine a mutually agreeable alternative to the use of such sub-subprocessor. If the parties are unable to reach a mutually agreeable resolution, and ADP decides to continue with the use of such sub-subprocessor, Client may terminate the affected WFM Services with no penalty.
11. Audits and Certifications. With respect to the processing of Client EEA Personal Data:
    a. Client or its independent third party auditor reasonably acceptable to ADP and Subcontractor (which shall not include any third party auditors who are either a competitor of ADP or Subcontractor or not suitably qualified or independent), may audit the control environment and security practices relevant to Client EEA Personal Data processed in connection with the WFM Services only if:
        i. ADP has not provided sufficient evidence of its compliance with the technical and organizational measures that protect the production systems of the WFM Services through providing either: (i) a certification as to compliance with ISO 27001 or other standards (scope as defined in the certificate); or (ii) a valid ISAE3402 and/or ISAE3000 or other SOC 1 or SOC 2 attestation report. Upon Client's request, audit reports and/or ISO certifications are available through ADP; or
        ii. An audit is formally requested by Client's data protection authority.

b. Any audit pursuant to (a) above will be subject to the following conditions:
    i. during Subcontractor's and ADP´s reasonable business hours;
    ii. upon no less than 45 days´ written notice;
    iii. may be carried out by Client or by an independent auditor designated by Client;
    iv. may be carried out only once per year; provided, however, that Client may conduct additional audits throughout the year on the basis on a request / inspection of a data protection authority or other regulatory body;
    v. at Client´s cost;
    vi. based on an audit plan agreed by the parties and which shall not permit the testing / audit of controls already the subject of the certifications and reports mentioned in (a) above, for example, the SOC 2 Type II report issued by Subcontractor.

Always Designing for People™

List of Sub-subprocessors

Name	Engagement	Country
Google Inc. 1600 Amphitheatre Parkway Mountain View, California 94043 USA	Cloud Hosting Provider	USA EU, Australia or Canada
Twilio Inc. 75 Beale St., Ste. 300 San Francisco, CA 94105 USA	Short Message Service (SMS) mobile network aggregator	USA
Boomi, LP Att: Boomi's Privacy Office, 1400 Liberty, Ridge Drive Chesterbrook, PA, 19087 USA	Integration / ETL	USA
Kronos Solutions India Private Limited B-5, 4th Floor, Tower 4, Okaya Towers, Sector 62, Noida 201301, India	Customer support	India
Okta, Inc. 100 First Street San Francisco, CA, 94105 USA	Auth0 by Okta: Cloud based authentication and identity governance platform	USA, EU, Australia or Canada (according to location of hosting)

Always Designing for People™

ATTACHMENT 4 – SECURITY MEASURES

1. **ISAE3402 / SSAE 18 (SOC 2) Audit**

Subcontractor shall have ISAE3402/SSAE 18 (SOC 1 and SOC 2) audits carried out each year for the purposes of an examination of the relevant controls with respect to the WFM Services. Such audits shall be carried out by an independent, certified third party and the resulting reports shall be provided to Client upon request. Subcontractor shall ensure the datacenter carries out its own SOC 2 audits and provide such reports to Client upon request.

2. **ISO 27001 Audit**

Subcontractor shall ensure the datacenter used to provide the service will continue to have its IT security management certified according to ISO 27001. The audits shall be carried out by an independent, certified third party and upon request, Subcontractor shall provide the certificate to Client.

3. **Security**

In addition to the audits by independent third parties, Subcontractor shall continuously carry out the further measures as described below in order to ensure the protection and integrity of the data and the availability of the application:

4.1. Infrastructure of the Data Center

Subcontractor and/or its sub-processor shall check the infrastructure of the data center continuously in order to identify any security vulnerabilities.

4.2. Vulnerability of the Data

Subcontractor shall maintain continuous monitoring activities on a daily, weekly, monthly and/or quarterly basis to determine that the controls of the SOC 2 program are operating to ensure the security, availability and confidentiality of Client Data.

4.3. Virus and Malware Scanning

Subcontractor shall ensure that a scanner from a renowned manufacturer shall be consistently operated with the latest scan patterns and signatures, and that the servers are regularly scanned and appropriate action taken promptly.

4.4. Patch Management

Through an automated process, Subcontractor shall distribute all patches, updates, and upgrades of operating systems (including the infrastructure components), middleware, or applications to all relevant components after they have been released by the manufacturer and tested by Subcontractor. Subcontractor shall manage the patching process prudently to assure that critical patches are applied in a timely manner consistent with the associated risk.

4.5. Security Documentations and Measures

Subcontractor shall maintain an organizational unit that is responsible for security and compliance issues; this unit shall develop, maintain, and operate an operating platform in order to ensure that there is a trusted platform which meets the SOC 2 criteria for security, availability, processing integrity, and confidentiality.

4.6. System Security

During the term of this Agreement, Subcontractor shall maintain and implement data security measures in order to protect Client Data from theft, unwanted dissemination, and unauthorized access. Client will be promptly informed once Subcontractor becomes aware of unauthorized access as well as any security control resulting in compromise of Client Data. At least the following measures shall be taken:

4.6.1. Firewalls

Subcontractor shall have industry standard firewall protection to secure all network, database, and computer systems which Subcontractor needs to provide the WFM Services. The firewalls shall be updated promptly upon release of new security patches or an update of the software of the firewall provider or its software supplier.

4.6.2. Detecting Attempts at Unauthorized Access

Subcontractor shall maintain a system to detect and prevent any unauthorized access and have appropriate alerting mechanisms to address any anomalies in traffic.

4.6.3. Encrypted Data Transfers

Subcontractor shall use industry standard encryption technology to encrypt data transfers between Subcontractor's servers and Client's front ends as well as the connections between Subcontractor' servers and the servers of Client or of a third party appointed by Client, as mutually agreed upon.

4.6.4. Encrypted Data Storage

Subcontractor shall encrypt Client Data industry standard technology. This shall include any and all information from Client, as well as Client's work results stored and managed by the service.

4.6.5 Malicious Code

The Service provided by Subcontractor shall not contain any computer code which, in any manner whatsoever, adversely affects the features of the Service. This means that the Service shall not, inter alia, contain any code which adversely affects program routines, enables front ends or servers to release information (e.g., viruses, Trojans, time bombs, worms, trap doors, etc.), or is capable of attacking, deleting, or destroying any other Client Data.

5. Access Controls

Access to all network components, servers, databases, computers, and software programs shall be protected by an authentication procedure that requires giving at least the user name and the password. Subcontractor shall implement technical controls to enforce a password policy consisting of a minimum number of characters and complexity, including requirements of alpha, numeric, upper case, lower case and/or special characters. Lockout periods shall be in effect for inactivity and unsuccessful password attempts. Passwords must be changed after 90 days, at the latest.

Privileged access shall be secured by means of a two-factor authentication and shall be defined by Subcontractor in such a manner as to ensure that the access authorizations are granted only to the extent necessary to perform the assigned role. In addition to role-based training, Contractor personnel shall participate in security awareness and privacy training, which addresses customer data handling, upon hire and annually thereafter. Any access to Subcontractor's systems shall be recorded along with the time of access and the activities carried out.

6. Physical Access Control

Subcontractor shall ensure that its data center sub-processor uses industry standard technology to ensure that only the appropriately authorized staff have access to those systems of Subcontractor that are used to provide the Service. This shall include at least the following

measures: visitor sign-ins, role-based access controls, limited access to the server rooms and to the alarm systems which report any unauthorized access.

7. Security Incident Management

Subcontractor shall maintain and apply security management procedures, including a detailed escalation and notification plan. In the event that Subcontractor becomes aware of any violation of the security controls or compromise of Client Data, Subcontractor shall so advise Client without delay. Subcontractor shall be obligated to promptly initiate adequate countermeasures and inform Client of the progress made with these measures.

8. Return to Operation/Business Continuity

During the term of the Agreement, Subcontractor shall maintain a plan for returning the data center and support sites to operation in the event of a disaster and present a summary of this plan at the request of Client. Upon Subcontractor's declaration of disaster Subcontractor shall implement said plan to the best of its ability to return the WFM Services to operation. Subcontractor shall annually test and review its business continuity plan, and update as necessary.

9. Continuous Service/Disaster Recovery

During the term, Subcontractor shall maintain a Disaster Recovery plan and present verification of this plan (via the SOC 2 reporting) at the request of Client. Subcontractor shall test this plan once a year and verify that the planned measures are effective, reviewed by management and improved where called for.